

A TRUE COPY

Mar 11, 2022

s/ Daryl Olszewski

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Information associated with Instagram accounts:

Instagram Name: kara_anothony

Instagram Unique Identifying Number: 45468103239

that are stored at premises controlled by Meta Platforms, Inc.

Case No. 22 MJ 24

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

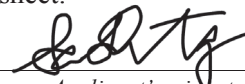
- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 2251(a)(2)	Attempted production of child pornography
18 U.S.C. 2251(a)	Production of child pornography
18 U.S.C. 2251(a)(5)(B)	Possession of child pornography

The application is based on these facts:

- ☐ Continued on the attached sheet.
- ☒ Delayed notice of 180 days (give exact ending date if more than 30 days: 09/05/2022) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



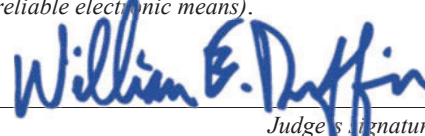
Applicant's signature

Sarah Dettmering, Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephone (specify reliable electronic means).

Date: 3/11/2022



Judge's signature

City and state: Milwaukee, WI

Honorable William E. Duffin

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Sarah Dettmering, being first duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Instagram account that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. (“Meta”), a company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta Platforms, Inc. to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the account.

2. I have been employed as a Special Agent of the Federal Bureau of Investigation (FBI), since January 2018, and am currently assigned to the Milwaukee Division as a member of the Milwaukee Child Exploitation and Human Trafficking Task Force. My duties include investigating criminal violations relating to child sexual exploitation and child pornography. While employed by the FBI, I have investigated federal criminal violations related to complex financial crimes, health care fraud, cybercrimes, child exploitation, and child pornography. I have received training from the FBI specific to investigating child pornography and child exploitation crimes and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256) in different forms of media including computer media. As a result of my training, experience, and discussions with other law enforcement officers assigned to investigate child pornography and child exploitation, I am familiar with methods by which electronic devices are

used as the means for receiving, transmitting, possessing, and distributing images and videos depicting minors engaged in sexually explicit conduct. I have also received training and gained experience in interview and interrogation techniques with enhanced training specific to cybercrimes, social media search warrants, residential search warrants, interviews and interrogations of subjects of criminal investigations, electronic device identification and forensic review, as well as sophisticated techniques used to commit cybercrimes.

3. The facts contained in this affidavit are known to me through my personal knowledge, training, and experience, and through information provided to me by other law enforcement officers, who have provided information to me during the course of their official duties and whom I consider truthful and reliable.

4. Based upon the information described below, I submit that probable cause exists to believe that the user of the Instagram Account in the name of “kara_anothony,” unique identifying number 45468103239, (SUBJECT ACCOUNT) has committed the crime of attempted production of child pornography, in violation of Title 18, United States Code, Section 2251(a)(2), production of child pornography in violation of Title 18, United States Code, Section 2251(a) and possession of child pornography in violation of Title 18, United States Code, Section 2252(a)(5)(B). I further submit that evidence relating to this crime, more particularly described in Attachment B, can be found in the contents of the SUBJECT ACCOUNT, more particularly described in Attachment A. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

DEFINITIONS

5. The following definitions apply to the Affidavit and Attachment B to this Affidavit:

a. “Child Pornography” is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

b. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. “An Internet Protocol address” (IP address) is a unique numeric address used by internet-enabled electronic storage devices to access the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that electronic storage device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some

computers have static that is, long-term IP addresses, while other computers have dynamic that is, frequently changed IP addresses.

e. “Minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

f. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

g. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

h. “Visual depictions” include undeveloped film and videotape, and data stored on a computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

i. “Website” consists of text pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up

Language (HTML) and is transmitted from the web servers to various web clients via Hyper-Text Transport Protocol.

BACKGROUND ON INSTAGRAM

6. Meta Platforms, Inc. (previously known as Facebook, Inc.) owns and operates a free-access social networking website, Instagram, that can be accessed at <http://www.instagram.com>. Instagram allows its users to establish accounts with Instagram, and users can then use their accounts to share written news, photographs, videos, and other information with other Instagram users, and sometimes with the general public. Instagram also links an Instagram Account to all of its Facebook accounts for its user to use.

7. Instagram operates a free-access social networking website that can be accessed at <http://www.instagram.com>. Instagram allows its users to establish accounts with Instagram, and users can then use their accounts to photographs, videos, post messages, and annotate messages with keywords with other Instagram users.

8. Instagram requires users to provide basic contact information to the company during the registration process. This information can include the user supplied name, contact e-mail addresses, telephone numbers, screen names, user profile image, and other personal identifiers.

9. Instagram records the creation date of every account. Additionally, the company records the Internet Protocol (IP) address of the computer or mobile device used to create the account. An IP address is roughly analogous to a telephone number and can be used to identify the Internet Service Provider (ISP) used by the person opening the account. Depending on the ISP, it may also be possible to resolve an IP address to a specific subscriber or device.

10. Instagram records and stores data they refer to as log file information. This includes the aforementioned IP addresses, internet browser type and version, referring domains or web pages, and the pages viewed by a user.

11. Instagram users can select two different levels of privacy for the communications and information associated with their Instagram accounts. Instagram accounts can be made viewable by anyone or restricted to other Instagram users who the account holder approves.

12. Instagram collects and retains information about the devices used to access their service. This can include the unique serial numbers of mobile devices such as the Mobile Equipment Identifier (MEID), the International Mobile Equipment Identifier (IMEI), the International Mobile Subscriber Identity (IMSI).

13. During the registration process an Instagram user is able to search for friends and associates through three different methods. If the user permits, the Instagram application will search through the contacts, or electronic address book, or a mobile device for other Instagram users. Instagram users may also elect to allow the application to search any associated Facebook accounts of the member for other users. An Instagram user may also manually search for friends or associates via the Instagram search feature. Instagram collects and stores the search history of its users.

14. Instagram users can post an unlimited number of digital images and videos to their account. These images may be taken from the internal storage of a mobile device or using the camera function of the Instagram application. The Instagram application prompts users to modify the images using free pre-defined filters and effects to change the appearance of the original image.

15. Instagram users are able to add keywords, referred to as hashtags and illustrated with the ‘#’ symbol, to their posted images and the posted images of others. These keywords represent search terms or comments making it easier for other users to seek and find material of interest to them.

16. Items posted to Instagram also have associated metadata that includes geotags marking the location an image was taken. The geotag information consists of the latitude and longitude where the image was taken. Geotag information is usually derived from the Global Positioning System (GPS) of a mobile device. An Instagram user must elect to use this feature.

17. Instagram users can send other user direct messages consisting of pictures or videos. Direct messages are visible only to the sender and recipient. The send of a direct message has control over the delivered image and can revoke it at any time. At the point the message is revoked by the sender it is no longer visible to the recipient.

18. As explained herein, information stored in connection with an Instagram account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, an Instagram user’s IP log, stored electronic communications, and other data retained by Meta Platforms Inc., can indicate who has used or controlled the Instagram account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, direct messaging logs, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Instagram account at a relevant time. Further, Instagram

account activity can show how and when the account was accessed or used. For example, as described herein, Meta Platforms, Inc. logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Instagram access, use, and events relating to the crime under investigation. Additionally, location information retained by Meta Platforms, Inc. may tend to either inculcate or exculpate the Instagram account owner. Last, Instagram account activity may provide relevant insight into the Instagram account owner's state of mind as it relates to the offense under investigation. For example, information on the Instagram account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

19. Therefore, the computers of Meta Platforms Inc. are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of Instagram, such as account access information, transaction information, and account application.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

20. On or about October 15, 2021 in an interview with the FBI, the parent of Victim 1 reported to the FBI that their child, who was a 16 year old male, had sent a sexually explicit image to the SUBJECT ACCOUNT. The user of the SUBJECT ACCOUNT then attempted to extort Victim 1 for \$300.

21. In the interview with the FBI Victim 1's parent disclosed that the SUBJECT ACCOUNT initially requested to follow Victim 1 on Instagram. Victim 1 accepted the follow request, and then received a message from the SUBJECT ACCOUNT via Instagram's direct messaging (DM). Victim 1 did not know the user of the SUBJECT ACCOUNT but saw that the SUBJECT ACCOUNT and Victim 1 followed some of the same accounts, this caused Victim 1 to believe that the user of the SUBJECT ACCOUNT was friends with some of Victim 1's friends. Victim 1's Instagram account was set to private, but Victim 1 disclosed to Victim 1's parent that they accepted any follow request that they received.

22. As described below, the SUBJECT ACCOUNT asked Victim 1 multiple times to send a nude image, and Victim 1 eventually complied.

23. The user of the SUBJECT ACCOUNT then sent multiple messages to Victim 1 threatening to send Victim 1's nude image to other Instagram accounts that Victim 1 followed, which included Victim 1's friends, unless Victim 1 sent the user \$300. Victim 1 did not send the money to the SUBJECT ACCOUNT and reported the incident to Victim 1's parent.

24. Victim 1's parent provided images taken of the Instagram DM exchange between Victim 1 and the SUBJECT ACCOUNT. The chats start on or about October 4, 2021 at approximately 6:57 PM, the captured chat exchange was initiated by the SUBJECT ACCOUNT. The images of the DM exchange provided to the FBI do not contain date and time stamps, however, Victim 1 reported the incident to Victim 1's parent on or about October 5, 2021. These chats between Victim 1 and the SUBJECT ACCOUNT via Instagram's DM occurred between October 4, 2021 and October 5, 2021.

25. Victim 1 had multiple images on his Instagram page which showed Victim 1 in a sport's uniform for Victim 1's high school. Once Victim 1 accepted the SUBJECT ACCOUNT as a follower, the user of the SUBJECT ACCOUNT was able to view the images on Victim 1's Instagram page.

26. The following exchange between Victim 1 (V1) and the SUBJECT ACCOUNT (SA) occurred via Instagram's direct messaging (DM) starting on or about October 4, 2021 at approximately 6:57 PM:

SA:	Hey [waving hand emoji]
V1:	Hi Wyd
SA:	I'm pretty good
V1:	What you doing
SA:	It's really bored what can we do to make our chat lively and fun [star eye emoji][star eye emoji]
V1:	Sure
SA:	Hmmmm don't you mind sneak pic exchange no [screen shot] with me and some fun [star eye emoji][heart eye emoji]

27. Later on in the DMs the following exchange took place between Victim 1 (V1) and the Subject Account (SA), where the SUBJECT ACCOUNT requests nude images multiple times from Victim 1:

V1:	[sends picture of a male with black pants and no shirt on, this is not V1. This is not CSAM. Male's face is not in the picture.]
SA:	Lol [laughing face emoji] It's not you
V1:	Ok [sends "disappearing message." This message appears as a gray box which states "Disappearing Message" this indicates that a message was sent but is not able to be viewed any longer] What do you look like
SA:	Hi no Used mirror pic ok
V1:	Ok

SA:	Good morning [smiling face emoji]
V1:	Good morning
SA:	What's up
V1:	Laying in bed Bouta take a shower
SA:	Used mirror pic now ok Then I will ok
V1:	[sends "disappearing message."]
SA:	I can't see you at all your dick with your face ok
V1:	U wanna dick pick?
SA:	Yes and your face ok Fully body nudes pics ok
V1:	Ok [Sends "disappearing message"] So Send me a full one
SA:	[Sends a screenshot of picture which has Victim 1's account name across the top and states "to you 7s" which indicates that this was the "disappearing message" that was sent to the SUBJECT ACCOUNT by Victim 1 seven seconds prior. This image shows Victim 1, a minor male, taking a picture in the mirror fully nude. Victim 1's penis is exposed in the image, and his face is visible.] [Sends a screenshot of Victim 1's Instagram page, which shows Victim 1's posted pictures and full name.] [Sends multiple screenshots of Victim 1's Instagram followers]
V1:	What
SA:	Hey I have ur nudes and everything needed to ruin your life, i have screenshot all ur followers and tags and those that comment on ur post. I can send this nudes to in Homercity pa til it go virals or send this all females on your list and your family if u don't cooperate... all u have to do is to cooperate with me and i will not expose u, if u block me i will ruin your life..

	Just cooperate with me ok
--	----------------------------------

28. The user of the SUBJECT ACCOUNT initially requested payment by stating:

SA	Are you ready to cooperate with me rn Pay me \$300 Fast response now ok
V1:	Fuck

29. The user of the SUBJECT ACCOUNT continued to attempt to force Victim 1 to send the user money via CashApp. A sample of the messages sent by the SUBJECT ACCOUNT to Victim 1 are below

SA:	I'm not joking with you ok Are you ready to cooperate with me rn
V1:	Yea
SA:	How much is with rn Fast response now ok
V1:	Venmo?
SA:	No cash app Give me your mobile number now ok Fast response now ok Just cooperate with me then we are good ok

SA:	Do you have a cash app Fast response now ok
V1:	Yea
SA:	How much are you going to send to me Fast response now ok Answer me now ok
V1:	I can't send 300
SA:	How much can you send to me
V1:	100
SA:	Ok Hold on now ok
V1:	Pls delete tho
SA:	Hey £ibddon92 Send it now ok and show m the screenshot now ok I will delete tho ok

	[Victim 1] fast response now ok What are you doing rn
--	--

SA:	Send it now ok and show me the screenshot now ok Fast response now ok
V1:	It's not letting me add my card anymore
SA:	Let me see the screenshot now ok
V1:	I don't ducking have it
SA:	What do you mean by that [SUBJECT ACCOUNT sent Victim 1 multiple screenshots of what appeared to be the SUBJECT ACCOUNT sharing Victim 1's nude image with Instagram accounts that followed Victim 1.¹]
V1:	Don't Fuck
SA:	Are you ready to cooperate with me now ok
V1:	Yes
SA:	Do what I say rn ok Then we are good Fast response now ok Are you crazy [Victim 1] Do you have any gift card at home Fast response now ok What are you doing rn Tell me the truth what's going on [Victim 1] I think you don't wanna cooperate with me ok I will expose you till it v I see you are very stubborn o I will let you down Just tell me how much do you have with you rn Don't lie to me ok let me know now

30. Subsequent to viewing the Instagram chats between Victim 1 and the SUBJECT ACCOUNT, I attempted to view the SUBJECT ACCOUNT on Instagram. A search of the name

¹ These alleged screenshots showed two separate Instagram DM conversations between the SUBJECT ACCOUNT and Victim 1's followers, the first message in these alleged screenshots was from the SUBJECT ACCOUNT to the follower and was the nude image of Victim 1. The SUBJECT ACCOUNT sent messages to Victim 1 implying that the images were distributed in order to get Victim 1 to stop being "stubborn" and comply with the SUBJECT ACCOUNT's request for money.

“kara_anothony” returned no accounts with an exact name match. I also attempted to find the account using the unique identifying number described in Attachment A, when this identifying number was searched on Instagram no search results were found.

31. Pursuant to an administrative subpoena, Meta Platforms, Inc. stated that as of October 6, 2021 the SUBJECT ACCOUNT was no longer active on Instagram. This indicates that the user of the SUBJECT ACCOUNT deactivated their account subsequent to the conversation with Victim 1.

32. Meta Platforms, Inc. was served with a preservation request for the SUBJECT ACCOUNT, therefore there is probable cause to believe that the information stored in the SUBJECT ACCOUNT will still be available despite the user deactivating the account.

33. Through my training and experience I know that if a subject solicits one victim for sexually explicit images and videos it is likely that the subject is also soliciting other victims. Therefore, there is probable cause to believe that the SUBJECT ACCOUNT will contain further messages, images, followers, or likes with other victims which are further evidence of violations of federal law as described in paragraphs above.

34. Based upon the factors presented, there is probable cause to believe that the contents of the SUBJECT ACCOUNT can assist law enforcement in identifying the user of the SUBJECT ACCOUNT, the actions of the user violating federal law, and further victims.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

35. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Meta to disclose to the government copies of the records and other information (including

the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

36. Based on the foregoing, I believe that probable cause exists that violations of Title 18, United States Code, Section 2251(a)(2), attempted production of child pornography, Title 18, United States Code, Section 2251(a), production of child pornography, and Title 18, United States Code, Section 2252(a)(5)(B), possession of child pornography have been committed by a user associated with the SUBJECT ACCOUNT, and that evidence of such violations exists in the SUBJECT ACCOUNT.

37. Because the warrant will be served on Meta Platforms, Inc. who will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

38. This Court has jurisdiction to issue the requested warrant because it is a “court of competent jurisdiction” as defined by 18 U.S.C § 2711. Specifically, the Court is “a district court of the United States ... that – has jurisdiction over the offense being investigated.” 18 U.S.C § 2711(3)(A)(i).

39. Pursuant to 18 U.S.C § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

40. The investigation of this criminal activity discussed above is ongoing, disclosure of the search warrant, this affidavit, or this application may result in the dissemination of these materials to the subject, who may destroy evidence, flee from prosecution, or otherwise evade the

investigation. Disclosure of the contents of this affidavit and related documents might have a significant and negative impact on the continuing investigation and might severely jeopardize its effectiveness.

41. I request that the Court order Meta Platforms, Inc. not to notify any person (including the subscribers or customers of the account listed in Attachment A) of the existence of the requested warrant for a period of twelve months, or until further order of the Court.

42. Meta Platforms, Inc. is a provider of an electronic communication service, as defined in 18 U.S.C. § 2510(15), and/or a remote computer service, as defined in 18 U.S.C. § 2711(2). Pursuant to 18 U.S.C. § 2703, I seek a warrant requiring Meta Platforms, Inc. to disclose records and information in connection with a criminal investigation. Accordingly, I respectfully request that the Court issue an order that the search warrant, this affidavit in support of the application for the search warrant, and the application for a search warrant be filed under seal until further order of this Court. Although the above documents may be sealed, it is respectfully requested that the data obtained as a result of the search warrant may be disclosed to third parties to facilitate analysis. For the foregoing reasons, I further respectfully request, pursuant to 18 U.S.C. § 2705(b) that the Court command through a Non-Disclosure Order that Meta Platforms, Inc. not notify any person of the existence of the requested warrants or the underlying investigation because such notification would seriously jeopardize the ongoing investigation.

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

This warrant applies to information associated with the following Instagram accounts:

Instagram Name: kara_anothony

Instagram Unique Identifying Number: 45468103239

that are stored, maintained, controlled, and administered by Meta Platforms, Inc. a company headquartered at Menlo Park, CA 94025.

ATTACHMENT B
INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. (“Meta”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Meta, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each user ID listed in Attachment A:

1) Messages, read or unread, maintained within the account, including stored or preserved copies of messages sent to and from the account, draft messages, deleted messages if available, the destination addresses associated with each message, the date and time at which each message was sent, and the size and length of each message, and any non-text or multimedia content sent with the messages; photos, videos, comments, and location information;

2) Any and all pictures/videos sent and/or received by the user, including visual depictions of sent and/or received files of visual depictions of sexually explicit conduct which has a child as one of its participants or portrayed observers in violation 18 U.S.C § 2251(a) and 18 U.S.C § 2252A(a)(2) or other computer graphic files which would indicate the ownership of computer media;

3) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them from September 1, 2021 to Present including

Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos;

- 4) Username, password, and email address upon registration of any existing accounts;
- 5) All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the Internet Protocol (“IP”) address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number), and any other records or information pertaining to the accounts;
- 6) All contact and personal identifying information, including: full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- 7) User Content, including, but not limited to, photos, comments, likes, Instagram searches, and other material posted to Instagram accounts;
- 8) Communication between SUBJECT ACCOUNT and Instagram, including account verification, changes/updates to features of Instagram, technical and security notices;
- 9) Evidence indicating the Instagram account owner's state of mind as it relates to the crime under investigation;
- 10) "Invite Friends" information, if available;

11) Information sent by device or Instagram, including visited webpages, add-ons, and other information collected by third-party analytics tools used in conjunction with Instagram and Facebook accounts;

12) All records of Instagram searches performed by the account from September 1, 2021 to Present;

13) Log file information reported by the browser, including, but not limited to, web request, Internet Protocol (IP) address, browser type, referring/exit pages and URLS, number of clicks and how the user interacted with links on Instagram, domain names, landing pages, pages viewed, and other information;

14) Device information, such as:

- a. Device Attributes: information such as the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins.
- b. Device Identifiers: unique identifiers, device IDs, and other identifiers, such as from games, apps or accounts used, and Family Device IDs (or other identifiers unique to Meta Platforms, Inc. associated with the same device or account).
- c. Device Signals: Bluetooth signals, and information about nearby Wi-Fi access points, beacons, and cell towers.
- d. Date from device settings: information received through device settings turned on, such as access to GPS location, camera or photos.

- e. Network and Connections: information such as the name of the mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, if available, information about other devices that are nearby or on the same network.
 - f. Cookie Data: data from cookies stored on the device, including cookie IDs and settings.
- 15) Metadata added to the user content including a hashtag, geotag, comments or other data;
- 16) The contents of all emails, other communications, or other information associated with the Subject Account described in Attachment A whether stored in the account, previously stored in the account, preserved by Meta on Meta's servers, or otherwise stored, maintained, controlled, or preserved by Meta and;
- 17) All "check ins" and other location information;
- 18) All records or other information stored at any time by any individual using the account, including contact and friend lists, calendar data, pictures, telephone numbers, physical addresses, to-do lists, links to other messages, websites, emails, or internet addresses, and other files;
- 19) All privacy settings and other account settings, including privacy settings for individual Instagram posts and activities, and all records showing which Instagram users have been blocked by the account;
- 20) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number)

21) All privacy settings and other account settings, including privacy settings for individual Instagram posts and activities, and all records showing which Instagram users have been blocked by the account;

22) Records relating to who created, used, or communicated with the user ID, including records about their identities and whereabouts.

Meta is hereby ordered to disclose the above information to the government within **fourteen days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of production of child pornography, in violation of Title 18, United States Code, Section 2251(a)(2), production of child pornography in violation of Title 18, United States Code, Section 2251(a) and possession of child pornography in violation of Title 18, United States Code, Section 2252(a)(5)(B) involving the SUBJECT ACCOUNT as described in Attachment A, since September 2021 including, for the user ID identified on Attachment A, information pertaining to the following matters:

- (a) Communications between the user of the SUBJECT ACCOUNT and minor victims;
- (b) Evidence indicating how and when the Instagram account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Instagram account owner;

- (c) Evidence indicating the Instagram account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.